NetBrain® Next-Gen R11.1b

Audit Log Streaming Setup

Version R11.1b | Last Updated 2025-03-18

Contents

1. Overview

Audit Log Streaming allows NetBrain to send audit logs in real-time to a 3rd party system such as Splunk for audit purposes or log analysis.

The following two types of logs can be streamed:

- Audit logs for user operations, which record all UI operations.
- Audit logs for device access, which record operations executed on devices in the Front server and/or using Smart CLI, including logins, logouts, executed commands, etc.

The supported streaming methods include:

- Webhook
- Syslog protocol:
  - Syslog TCP (RFC 5424). Send the Syslog message over TCP using the RFC 5424 format.
  - Syslog UDP(RFC 5424). Send the Syslog message over UDP using the RFC 5424 format.
  - Syslog TCP with TLS (RFC 5424). Send the Syslog message over TCP with TLS encryption using the RFC 5424 format.

Select an option to set up log streaming based on your requirements and preferred network protocol:

- Set up log streaming with a webhook.
- Set up Log Streaming with Syslog.

2. Set Up Log Streaming with Webhook

Follow the steps to set up audit log streaming:

1. Integrate a third-party system with webhook.
2. Enable log streaming in the NetBrain system

2.1. Integrate a Third-Party System with Webhook

We will use Splunk and LogStash (most often used as a data pipeline for Elasticsearch) as examples. Contact the NetBrain support team if you use another 3rd party system or do not know how to set up the system.

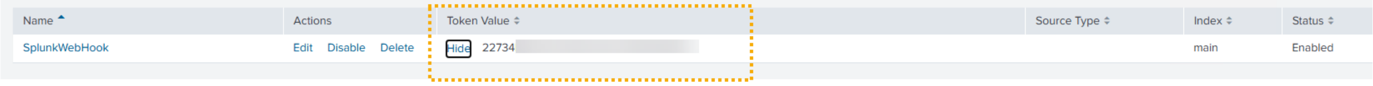
1.2.1.Example 1: Integrate Splunk HTTP Event Collector with Webhook

Follow the steps to set up Splunk HTTP Event Collector and configure a webhook.

1. Set up Splunk HTTP Event Collector to receive the audit logs.
2. Add an outgoing webhook to send the audit logs.

Set up Splunk HTTP Event Collector

1. Configure the HTTP Event Collector.
   - For Splunk Web: Check Configure HTTP Event Collector on Splunk Cloud Platform and refer to the below sections:
     i. Enable HTTP Event Collector on the Splunk Cloud Platform
     ii. Create an Event Collector token on the Splunk Cloud Platform
   - For Splunk Enterprise: Check Configure HTTP Event Collector on Splunk Enterprise and refer to the below sections:
     i. Enable HTTP Event Collector on Splunk Enterprise
     ii. Create an Event Collector token on Splunk Enterprise
2. Document the token value, as it will be required when adding the outgoing webhook.

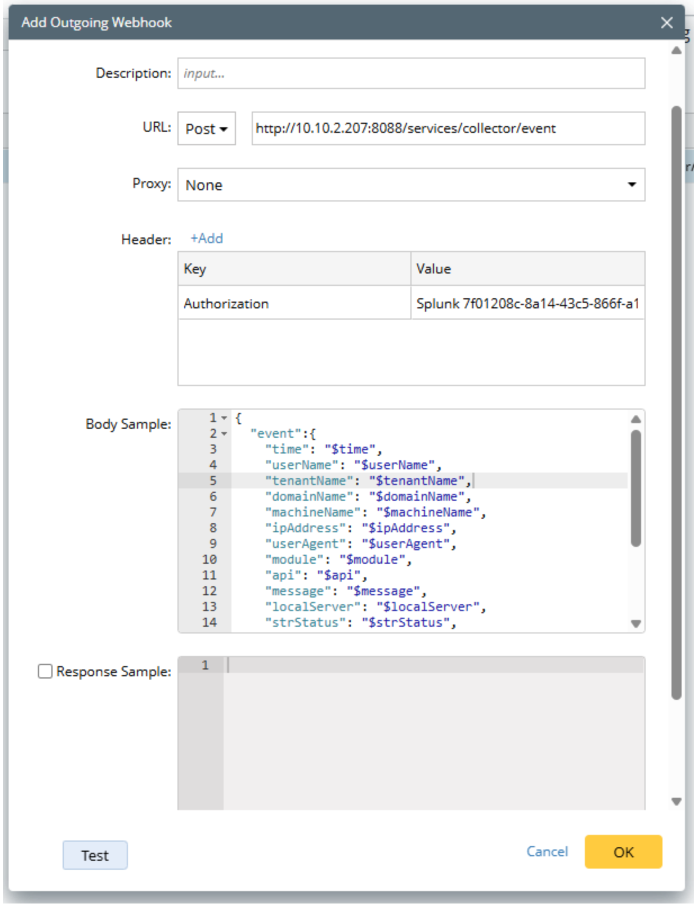


Name	Actions	Token Value	Source Type	Index	Status
SplunkWebHook	Edit Disable Delete	Hide 22734[redacted]		main	Enabled

Add Outgoing Webbook in NetBrain System

1. Log in to the NetBrain System Management page.
2. Click the start menu and select **Add Outgoing Webhook** from the drop-down menu.

3. In the **Add Outgoing Webhook** window, define a webhook for HTTP Event Collector.



Description: input...

URL: Post ▾ http://10.10.2.207:8088/services/collector/event

Proxy: None ▾

Header:

Key	Value
Authorization	Splunk 7f01208c-8a14-43c5-866f-a1

Body Sample:

```
{
  "event":{
    "time": "$time",
    "userName": "$userName",
    "tenantName": "$tenantName",
    "domainName": "$domainName",
    "machineName": "$machineName",
    "ipAddress": "$ipAddress",
    "userAgent": "$userAgent",
    "module": "$module",
    "api": "$api",
    "message": "$message",
    "localServer": "$localServer",
    "strStatus": "$strStatus",
```

□ Response Sample:

a. Define basic information about the outgoing webhook, including Name and Description.

b. In the URL block, select **Post** as the method, then input http://<The IP address hosting Splunk: port number>/services/collector/event.

c. Add a Header by clicking **+Add**.

   i. Enter **Authorization** as Key.

   ii. Enter the token value recorded in Set up Splunk HTTP Event Collector.

d. In the Body Sample, paste the sample below. (Refer to Parameters and Sample Log for more details.)

Sample

```
{

  "event":{

    "time": "$time",

    "userName": "$userName",

    "tenantName": "$tenantName",

    "domainName": "$domainName",

    "machineName": "$machineName",
    "ipAddress": "$ipAddress",
    "userAgent": "$userAgent",
    "module": "$module",
    "api": "$api",
    "message": "$message",
    "localServer": "$localServer",
    "strStatus": "$strStatus",
    "status": "$status",
    "deviceName": "$deviceName",
    "deviceIp": "$deviceIp",
    "deviceUser": "$deviceUser",
    "command": "$command",
    "taskType": "$taskType",
    "Error": "$Error"
}}
```

Parameters

Parameter	Description	Example	Audit Log Type
$time	The timestamp	**2025-03-25T03:16:45.46Z**	• User Operation • Device Access
$userName	The username in the NetBrain system	**admin**	• User Operation • Device Access
$tenantName	The tenant name in the NetBrain system	**Initialize Tenant**	• User Operation • Device Access
$domainName	The domain name in the NetBrain system	**Demo Domain**	• User Operation • Device Access
$machineName	• User Operation Log: The computer name where the browser was running.	**BJDG317-000036**	• User Operation • Device Access

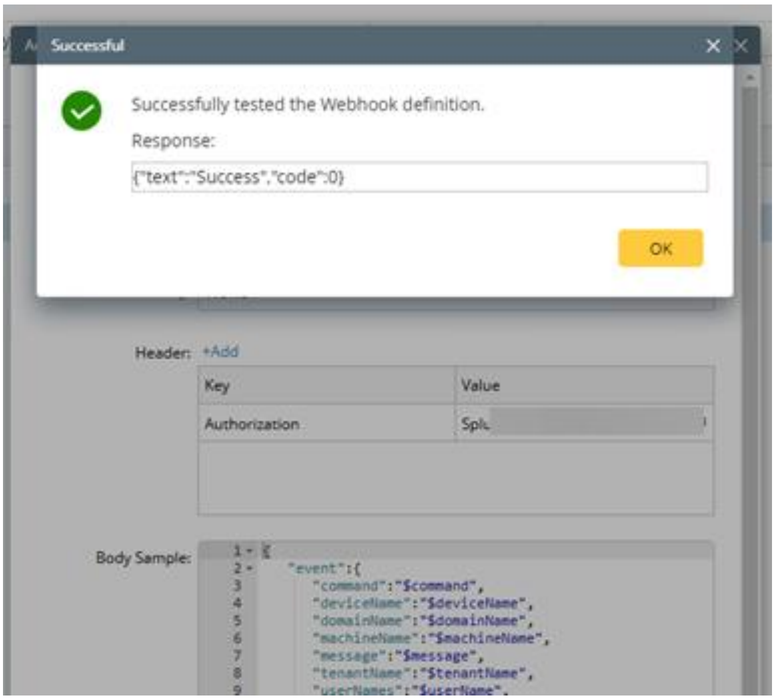
Parameter	Description	Example	Audit Log Type
	• Device Access Log: The machine where the Front Server is installed. It is the same as the **`$localServer`**.		
$ipAddress	The IP address of the computer where the browser was running.	`10.10.0.1`	User Operation
$userAgent	The browser vendor used by the user	`Chrome`	User Operation
$module	Web Server module	`Login`	User Operation
$api	Web Server API	`Login`	User Operation
$message	Log message	`Log in to End User Page with username admin.`	• User Operation • Device Access
$localServer	The computer where Web Server or Front Server is installed.	`BJDG317-000036`	• User Operation • Device Access
$status	Status codes There are three status codes: 0: Success 1: Failed 2: Exception	`0`	User Operation
$strStatus	The string name of the status	`Success`	User Operation
$deviceName	Accessed device	`BJ*POP`	Device Access

Parameter	Description	Example	Audit Log Type
$deviceIp	The IP address of the accessed device	`172.24.255.8`	Device Access
$deviceUser	The user who accessed the device	`admin`	Device Access
$command	The command executed to access the device	`show interface`	Device Access
$taskType	Task type for device access. • DTG: data task group • DLA: direct live access	`DLA`	Device Access
$Error	Error description		User Operation

Sample Log

```
{

  "event":{

    "time": "2025-03-24T09:09:58.986Z",

    "userName": "admin",

    "tenantName": "Initialize Tenant",

    "domainName": "Demo Domain",

    "machineName": "BJDG317",

    "ipAddress": "172.24.255.8",

    "userAgent": "$userAgent",

    "module": "Logout",

    "api": "Logout",

    "message": "Log out from End User Page due to session timeout.",

    "localServer": "BJDG317",

    "strStatus": "Success",
    "status": 0,

    "deviceName": "BJ*POP",

    "deviceIp": "172.24.255.8",

    "deviceUser": "admin",

    "command": "show interface",

    "taskType": "DLA",

    "Error": ""

}}
```

4. (Optional) Click **Test** to test the webhook.



Successfully tested the Webhook definition.

Response:

{"text":"Success","code":0}

Key	Value
Authorization	Spl[redacted]

Body Sample:

```
{
    "event":{
        "command":"$command",
        "deviceName":"$deviceName",
        "domainName":"$domainName",
        "machineName":"$machineName",
        "message":"$message",
        "tenantName":"$tenantName",
        "userNames":"$userName",
```

After the webhook passes the test, click **OK** to save the webhook.

1.2.2.Example 2: Integrate LogStash service with Webhook

Follow the steps to set up the Logstash service and configure a webhook.

1. Set up LogStash to receive the audit logs.
2. Add an outgoing webhook to send the audit logs.

Install and Configure LogStash

1. Install LogStash on a server that will receive the logs.
2. In the `/etc/logstash/conf.d/` directory, create a pipeline configuration file, defining the Logstash processing pipeline.

Example: Create and modify the config file **logstash1.conf.**

```
[root@localhost]# vi /etc/logstash/conf.d/logstash1.conf

input {
  http {
   host => "0.0.0.0"
   port => 5044
  }
}

output {
  file {
    path => "/tmp/logstash_output.log"
    codec => json_lines
  }
}
```

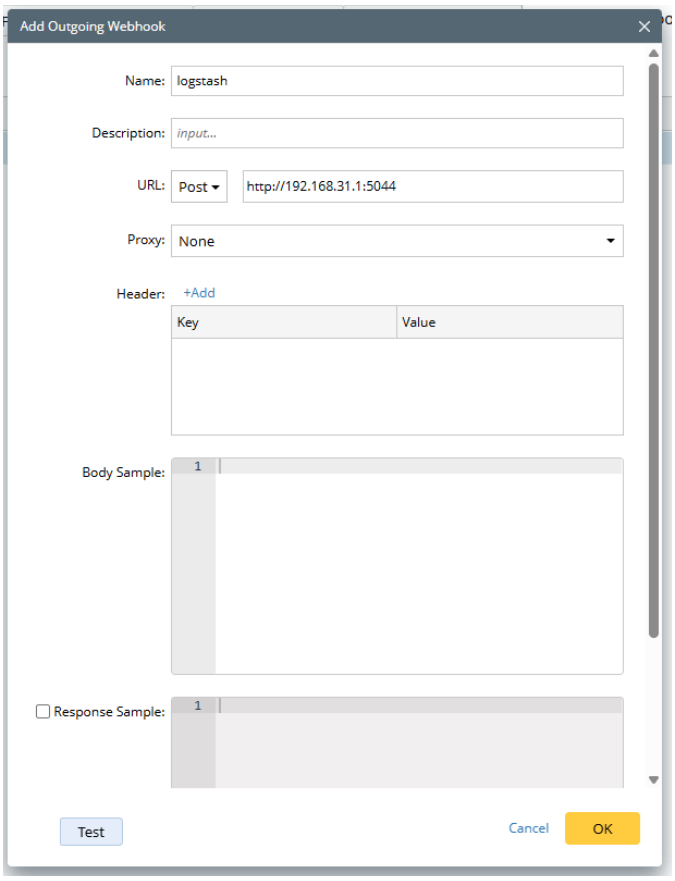
- This config file uses the **inputs** and **outputs** plugins.
- **Input**: It receives events over HTTP or HTTPS/ uses 0.0.0.0 as a host IP address and port 5044 to communicate.
- **Outpu**t: The file path to write to is `/tmp/logstash_output.log`. The code used for output data is the default value `json_lines`.

3. Start the LogStash service by running the `systemctl start logstash.service` command.
4. Turn off the firewall on the internal network or add the port number to the exception list.

Add Outgoing Webbook in NetBrain System

1. Log in to the NetBrain System Management page.
2. Click the start menu and select **Add Outgoing Webhook** from the drop-down menu.

3. In the **Add Outgoing Webhook** window, define a webhook for Logstash.



Name: logstash

Description: input...

URL: Post http://192.168.31.1:5044

Proxy: None

a. Define basic information about the outgoing webhook, including Name and Description.

b. In the URL block, select **Post** as the method, then input http://<The IP address hosting Logstash: port number>.

e. (Optional for LogStash) In the Body Sample, paste the sample below to exclude irrelevant data fields, such as `userId`, `domainId`, or `tenantId`. (Refer to Parameters and Sample Log for more details.)

Skip this optional step if you want to include all date fields.

Sample

```
{

    "time": "$time",

    "userName": "$userName",

    "tenantName": "$tenantName",

    "domainName": "$domainName",

    "machineName": "$machineName",

    "ipAddress": "$ipAddress",

    "userAgent": "$userAgent",
    "module": "$module",

    "api": "$api",

    "message": "$message",

    "localServer": "$localServer",

    "strStatus": "$strStatus",

    "status": "$status",

    "deviceName": "$deviceName",

    "deviceIp": "$deviceIp",

    "deviceUser": "$deviceUser",

    "command": "$command",

    "taskType": "$taskType",

    "Error": "$Error"

}
```

Parameters

Parameter	Description	Example	Audit Log Type
$time	The timestamp	`2025-03-25T03:16:45.46Z`	- User Operation - Device Access
$userName	The username in the NetBrain system	`admin`	- User Operation - Device Access
$tenantName	The tenant name in the NetBrain system	`Initialize Tenant`	- User Operation - Device Access
$domainName	The domain name in the NetBrain system	`Demo Domain`	- User Operation - Device Access
$machineName	- User Operation Log: The computer name where the browser was running. - Device Access Log: The machine where the Front Server is installed. It is the	`BJDG317-000036`	- User Operation - Device Access

Parameter	Description	Example	Audit Log Type
	same as the **`$localServer`**.		
$ipAddress	The IP address of the computer where the browser was running.	**`10.10.0.1`**	User Operation
$userAgent	The browser vendor used by the user	**`Chrome`**	User Operation
$module	Web Server module	**`Login`**	User Operation
$api	Web Server API	**`Login`**	User Operation
$message	Log message	**`Log in to End User Page with username admin.`**	- User Operation - Device Access
$localServer	The computer where Web Server or Front Server is installed.	**`BJDG317-000036`**	- User Operation - Device Access
$status	Status codes There are three status codes: 0: Success 1: Failed 2: Exception	**`0`**	User Operation
$strStatus	The string name of the status	**`Success`**	User Operation
$deviceName	Accessed device	**`BJ*POP`**	Device Access
$deviceIp	The IP address of the accessed device	**`172.24.255.8`**	Device Access

Parameter	Description	Example	Audit Log Type
$deviceUser	The user who accessed the device	`admin`	Device Access
$command	The command executed to access the device	`show interface`	Device Access
$taskType	Task type for device access. • DTG: data task group • DLA: direct live access	`DLA`	Device Access
$Error	Error description		User Operation

Sample Log

```
{
    "time": "2025-03-24T09:09:58.986Z",
    "userName": "admin",
    "tenantName": "Initialize Tenant",
    "domainName": "Demo Domain",
    "machineName": "BJDG317",
    "ipAddress": "172.24.255.8",
    "userAgent": "$userAgent",
    "module": "Logout",
    "api": "Logout",
    "message": "Log out from End User Page due to session timeout.",
    "localServer": "BJDG317",
    "strStatus": "Success",
    "status": 0,
    "deviceName": "BJ*POP",
    "deviceIp": "172.24.255.8",

    "deviceUser": "admin",

    "command": "show interface",

    "taskType": "DLA",

    "Error": ""

}
```

4. (Optional) Click **Test** to test the webhook.

5. After the webhook passes the test, click **OK** to save it.

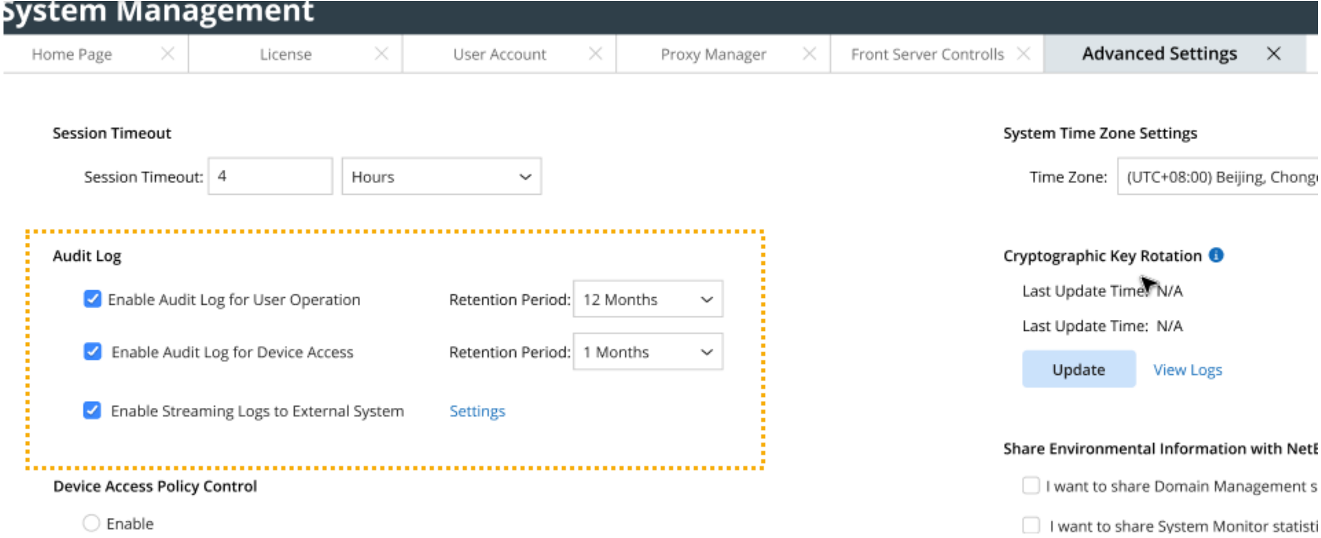
2.2. Enable Log Streaming in the NetBrain System

Follow the steps to enable streaming logs.

1. Log in to NetBrain system > **System Management** page.

2. Click the start menu and select **Advanced Settings** from the drop-down menu.

3. On the **Advanced Settings** tab, define the settings for log streaming.



Session Timeout

Session Timeout: 4 Hours

Audit Log

☑ Enable Audit Log for User Operation Retention Period: 12 Months

☑ Enable Audit Log for Device Access Retention Period: 1 Months

☑ Enable Streaming Logs to External System Settings

Device Access Policy Control

○ Enable

System Time Zone Settings

Time Zone: (UTC+08:00) Beijing, Chong

Cryptographic Key Rotation

Last Update Time: N/A

Last Update Time: N/A

Update View Logs

Share Environmental Information with NetE

□ I want to share Domain Management s

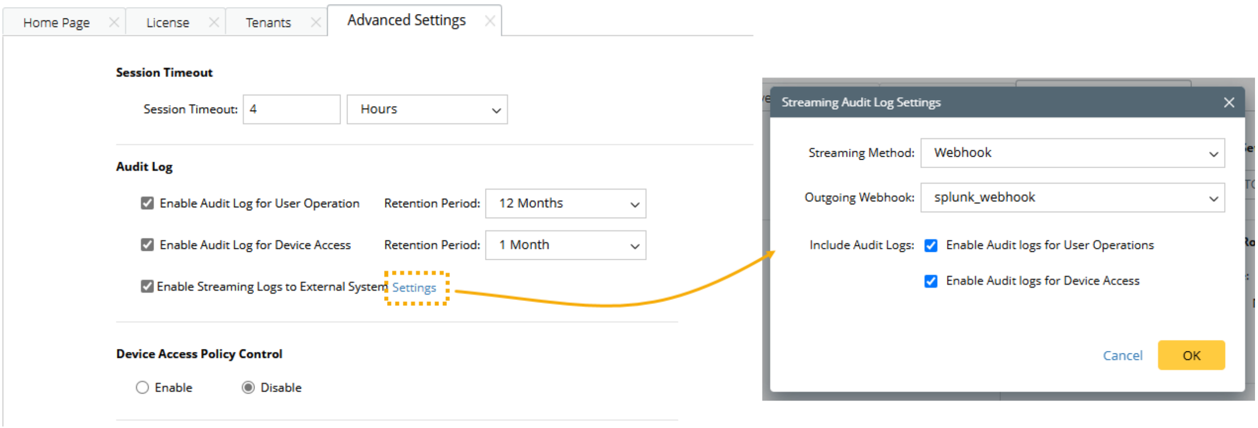
□ I want to share System Monitor statisti

a. Enable the checkbox **Enabled Audit Log for User Operation** to allow the NetBrain system to generate user operation logs.

b. Enable the checkbox **Enabled Audit Log for Device Access** to allow the NetBrain system to generate device access logs.

c. Enable the checkbox **Enable Streaming Logs to External System** to allow the NetBrain system to send logs to an external system.

d. Click **Settings** to select the webhook and which audit log to include.



Session Timeout

Session Timeout: 4 Hours

Audit Log

☑ Enable Audit Log for User Operation Retention Period: 12 Months

☑ Enable Audit Log for Device Access Retention Period: 1 Month

☑ Enable Streaming Logs to External System Settings

Device Access Policy Control

○ Enable ● Disable

Streaming Audit Log Settings

Streaming Method: Webhook

Outgoing Webhook: splunk_webhook

Include Audit Logs: ☑ Enable Audit logs for User Operations

☑ Enable Audit logs for Device Access

- In the **Streaming Audit Log Settings** window, select the outgoing webhook defined for the log receiver.
- Select the option(s) to be included in the streaming logs:
  - **User Operation**
  - **Device Access**
- Click **OK** to save the settings.

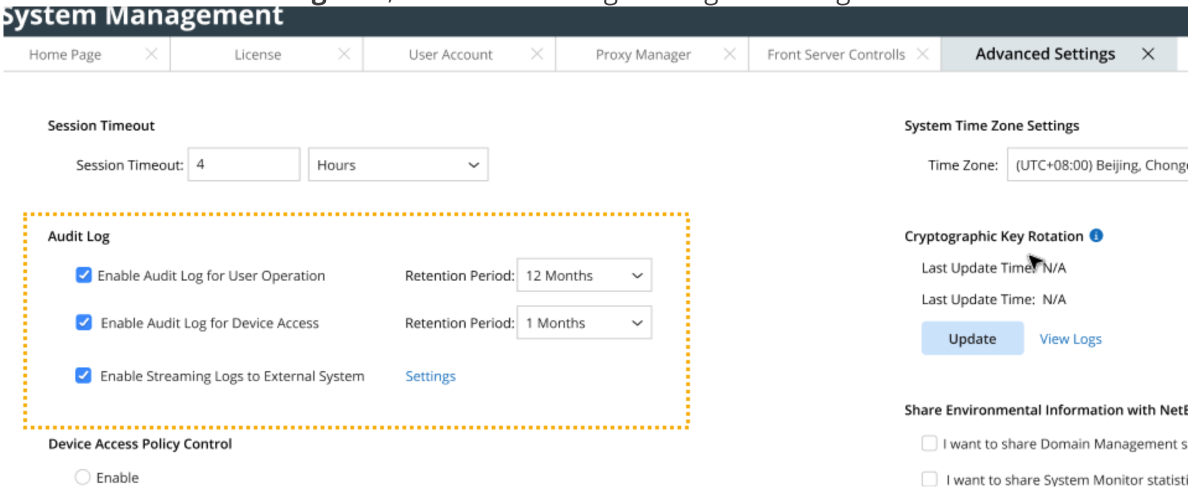
3. Set Up Log Streaming with Syslog

After preparing and setting up the Syslog server, follow the steps to enable streaming logs.

1. Log in to the NetBrain system > **System Management** page.

2. Click the start menu and select **Advanced Settings** from the drop-down menu.

3. On the **Advanced Settings** tab, define the settings for log streaming.



Session Timeout

Session Timeout: 4 Hours

Audit Log

☑ Enable Audit Log for User Operation Retention Period: 12 Months

☑ Enable Audit Log for Device Access Retention Period: 1 Months

☑ Enable Streaming Logs to External System

Device Access Policy Control

○ Enable

System Time Zone Settings

Time Zone: (UTC+08:00) Beijing, Chong

Cryptographic Key Rotation

Last Update Time: N/A

Last Update Time: N/A

Share Environmental Information with NetE

□ I want to share Domain Management s

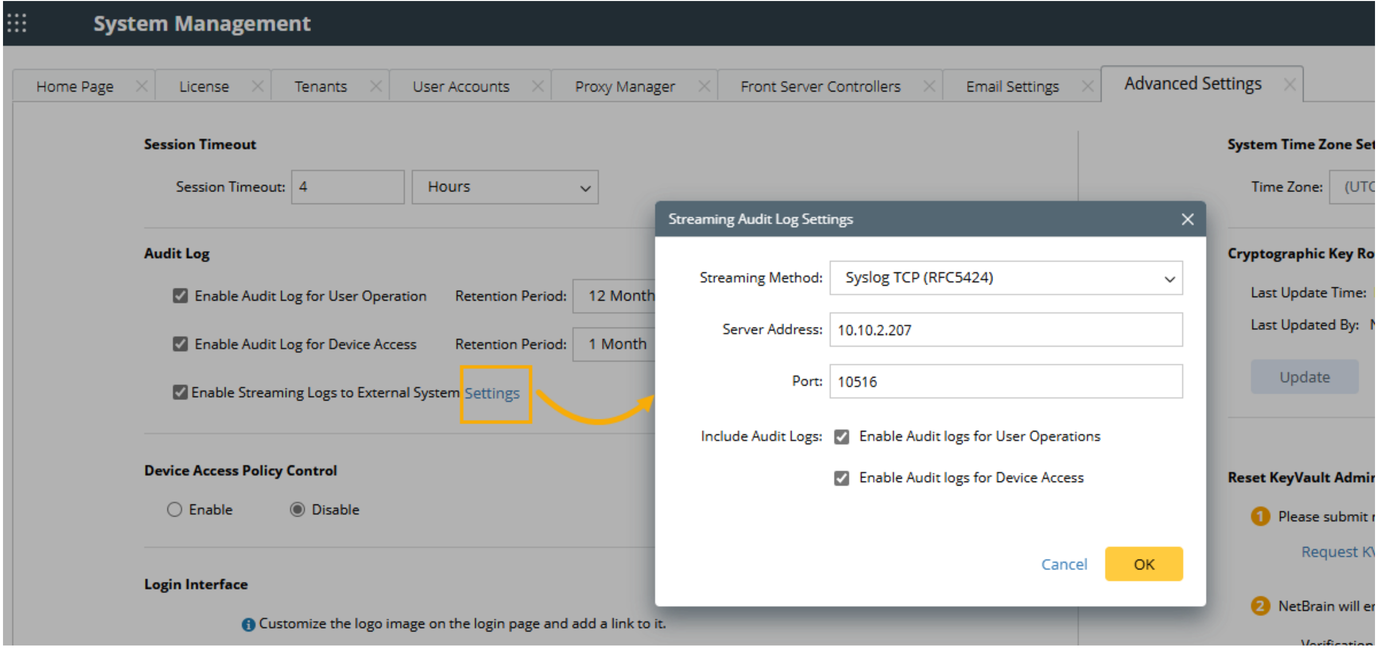
□ I want to share System Monitor statisti

a. Enable the checkbox **Enabled Audit Log for User Operation** to allow the NetBrain system to generate user operation logs.

b. Enable the checkbox **Enabled Audit Log for Device Access** to allow the NetBrain system to generate device access logs.

c. Enable the checkbox **Enable Streaming Logs to External System** to allow the NetBrain system to send logs to an external system.

4. Click **Settings** to define settings to communicate with the Syslog server.



Session Timeout

Session Timeout: 4 Hours

Audit Log

☑ Enable Audit Log for User Operation Retention Period: 12 Month

☑ Enable Audit Log for Device Access Retention Period: 1 Month

☑ Enable Streaming Logs to External System Settings

Device Access Policy Control

○ Enable ● Disable

Login Interface

Customize the logo image on the login page and add a link to it.

System Time Zone Set

Time Zone: (UTC

Cryptographic Key Ro

Last Update Time:

Last Updated By: N

Reset KeyVault Admir

1 Please submit r

Request K

2 NetBrain will er

Streaming Audit Log Settings

Streaming Method: Syslog TCP (RFC5424)

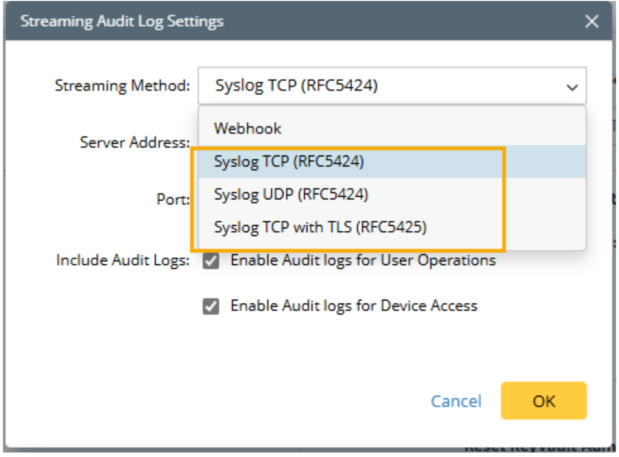
Server Address: 10.10.2.207

Port: 10516

Include Audit Logs: ☑ Enable Audit logs for User Operations

☑ Enable Audit logs for Device Access

A. In the **Streaming Audit Log Settings** window, select an option based on your transport protocol.



Streaming Audit Log Settings

Streaming Method: Syslog TCP (RFC5424)

Server Address:

Port:

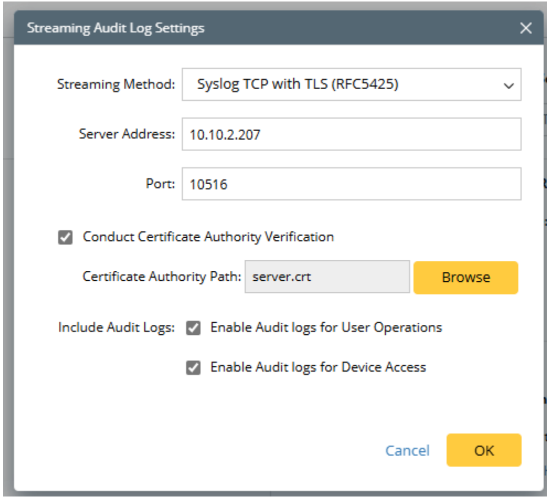
Include Audit Logs: ☑ Enable Audit logs for User Operations

☑ Enable Audit logs for Device Access

B. Enter the Syslog server address.

C. Specify the port that the Syslog server listens on.

D. (For TLS protocol) Enable the **Conduct Certificate Authority Verification** checkbox, and upload the certificate.



Streaming Audit Log Settings

Streaming Method: Syslog TCP with TLS (RFC5425)

Server Address: 10.10.2.207

Port: 10516

☑ Conduct Certificate Authority Verification

Certificate Authority Path: server.crt

Include Audit Logs: ☑ Enable Audit logs for User Operations

☑ Enable Audit logs for Device Access

E. Select the option(s) to be included in the streaming logs:

- **User Operation**
- **Device Access**

F. Click **OK** to save the settings.

Syslog Message Sample

- User Operation Logs

```
<110>1 2025-05-12T20:18:09.606074-07:00 WIN-A3J7D6NOS60 WebServer 1316 - [meta
userName="admin" tenantName="" domainName="" machineName="BJDG317-000036"
ipAddress="10.10.0.36" userAgent="Chrome" module="Login" api="Login"
strStatus="Succeeded" Error=""] Log in to End User Page with username admin.
```

- Device Access Sample:

```
<110>1 2025-05-13T03:33:23.430000+00:00 WIN-A3J7D6NOS60 FrontServer 10308 - [meta
userName="admin" tenantName="Initial Tenant" domainName="Beijing" machineName="WIN-
A3J7D6NOS60" deviceName="F5-SW2" deviceIp="172.25.124.4" deviceUser="nb"
command="terminal length 0"] Execute command "terminal length 0" on device F5-SW2.
```

Message Component	Example
The Priority value. It's the combination of facility and severity.	`110` Facility: 11 Severity: 0
The version number of the Syslog protocol	`1`

The timestamp	`2025-05-12T20:18:09.606074-07:00`
The hostname of the server generating the logs	`WIN-A3J7D6NOS60`
The application or process generating the message	• `WebServer` (User Operation Logs) • `FrontServer` (Device Access Logs)
The process ID	`1316`
Structured Data	`[meta userName="admin" tenantName="" domainName="" machineName="BJDG317-000036" ipAddress="10.10.0.36" userAgent="Chrome" module="Login" api="Login" strStatus="Succeeded" Error=""]`
The message body	`Log in to End User Page with username admin.`